



**Exhibit to Data Center Services
Service Component Provider
Master Services Agreement**

DIR Contract No. DIR-DCS-SCP-MSA-002

Between

**The State of Texas, acting by and through
the Texas Department of Information Resources**

and

**Atos IT Governmental Outsourcing Services, LLC (formerly called
XBS Disposition Subsidiary Two, LLC)**

**Appendix 5 to Eleventh Amendment
of**

**Exhibit 2.3
Server Services – Fully Managed
Statement of Work**

May 31, 2016

TABLE OF CONTENTS

A.0	SERVICE REQUIREMENTS	6
A.1	Operations	6
A.1.1	Physical Security Administration.....	9
A.2	Production Control and Scheduling	10
A.3	Technical Support	11
A.3.1	General Technical Support.....	11
A.3.2	Capacity and Performance Management	13
A.3.3	Systems Management	13
A.4	Database Support and Management.....	14
A.4.1	Database Management	14
A.4.2	Database Maintenance and Support	14
A.4.3	Database Administrative Support	15
A.5	Online Storage and Backup Management.....	16
A.5.1	Storage and Backup Architecture.....	16
A.5.2	Engineering	16
A.5.3	Operations and Processing	17
A.5.4	Backup and Recovery Services	18
A.5.5	Administration	18
A.6	External Storage Media Management – (Consolidated)	19
A.6.1	Operations and Processing	19
A.6.2	Administration	19
A.6.3	Off-Site Media Storage Management	20
A.7	External Storage Media Management – (Non-Consolidated)	20
A.7.1	Operations and Processing	20
A.7.2	Administration	21
A.7.3	Off-Site Media Storage Management	21
A.8	Authorized User Support	23
A.9	Intrusion Prevention.....	23
A.10	Consolidated and Non-Consolidated Data Center Email Services	23
A.10.1	Email – Procedures	23
A.10.2	Email – Technical Support.....	24
A.10.3	Email – Operations.....	25
A.10.4	Authorized User Support	25
A.11	Enhanced Security Hosted Email Services	26

EXHIBIT 2.3

SERVER SERVICES STATEMENT OF WORK

Update Methodology to Exhibit 2.3

The following update methodology is incorporated as part of Exhibit 2.3:

Title	Methodology for Updating Exhibit
<u>Exhibit 2.3</u> Server Services Fully Managed SOW	<u>Exhibit 2.3</u> may only be modified by formal amendment, in accordance with <u>Section 21.7</u> of the MSA.

Introduction

Service Provider will provide a solution that supports all of the business processes described in this Statement of Work and its Attachments, and that all Services, unless otherwise specifically stated, are included in the Charges.

Service Provider will be responsive to the current and future requirements of DIR and DCS Customers, by proactively anticipating needs, and adjusting Services accordingly within the Charges. Requirements for New Services will be handled in accordance with **Section 11.5** of the Agreement and Service Provider will work with DIR to assess the impact of these requirements on DIR's and DCS Customers' operating environment and supported Applications in accordance with the terms of the Agreement.

This Exhibit sets forth the Services that the Service Provider will provide, as of the Commencement Date unless otherwise specified, for all Services that affect Application and Utility Servers described in this Exhibit.

The Service Provider is also required to provide the Services in **Exhibit 2.1.2** in conjunction with the Services described in this Exhibit.

Service Management

DIR bases its Service Management practices on the Information Technology Infrastructure Library (ITIL), a world-wide recognized best-practice framework for the management and delivery of IT services throughout their full life-cycle. Accordingly, DIR requires that Service Provider Service Management practices, which are used to support the Services, be based on the ITIL framework and guidance. The primary structure of the requirements in the Statements of Work are based on an ITIL v2 foundation with ITIL v3 guidance in select functional areas (e.g. Request Management and Fulfillment) with the expectation of migrating towards ITIL v3 progressively as process improvements are incorporated into the Service Management Manual.

Service Provider responsibilities include:

1. Intentionally deploy and actively manage a set of Service support processes and Service delivery processes that are based on ITIL guidance to enable consistent management of process-driven IT services seamlessly across a variable number of environments and among DCS Service Providers.

2. Ensure that ITIL-based processes effectively integrate with the processes, functions and roles deployed within and used by DIR and DCS Customers and other DCS Service Providers.
3. Execute detailed activities and tasks that are common to IT service operation and maintenance according to the guidance set out in the policies and procedures described in **Exhibit 2.1.2**, including the broader guidance provided regarding the ITIL-based Service Management processes.
4. Design processes to enable the effective monitoring and reporting of the IT services in a Multi-Supplier Environment. Ensure that enterprise processes (e.g. Change Management, Configuration Management, Problem Management) are followed across the DCS Service Provider and Third Party Vendor(s) processes.
5. Coordinate the execution of all the processes across the Service Provider, DIR, DCS Customers, and all Service Component Providers in order that all the individual components that make up the IT Services are managed in an end-to-end manner.

A.0 SERVICE REQUIREMENTS

All activities required to provide the Services set forth in this SOW, including project-related support activities, are included in the Charges.

A.1 Operations

Service Provider responsibilities include:

1. Assume responsibility for the following requirements associated with Application, Utility and Infrastructure Servers, regardless of the physical location of the Equipment, whether located in a Consolidated Data Centers, Cloud Service Provider locations or Non-Consolidated remote locations.
2. Assume responsibility for all master and subordinate console functions.
3. Issue operator commands to control all In-Scope computer platforms throughout the organization.
4. Assume the responsibility for and perform all console operations:
 - 4.1. Install, monitor and support tools for the collection of detailed information required for SLAs, Reports and Invoicing.
 - 4.2. Service Provider will ensure the implementation of hardware system management and monitoring for servers in the Consolidated Data Centers and as requested by DIR.
 - 4.3. Manage and monitor server performance and utilization of the various server resources necessary to provide optimum Services performance (e.g. CPU, file system level storage, memory, server network interface throughput).
 - 4.4. Monitor all processing.
 - 4.5. Monitor the performance of online interactive traffic and take appropriate action to resolve online-system-related incidents and/or problems, including escalating (as appropriate) the incident and/or problem to the proper Level 2 Support group.
 - 4.6. Monitor and ensure the successful transmission of files between Consolidated Data Centers, Cloud Service Provider locations, Non-Consolidated remote locations or any other parties designated by DIR.
5. Provide operational support for data transmission (send/receive), consistent with commercial or DIR Standards (e.g. FTP or Managed File Transfer software products).
6. Manage, maintain, monitor, and control online and batch process, both scheduled and unscheduled (including on-request processing).
7. Complete DCS Customer defined batch processing and backups and restores in the correct sequence and within the time periods designated by DIR and DCS Customers.
8. Schedule batch jobs within DIR and DCS Customer defined windows to achieve maximum performance as long as required batch completion times are met.
9. Where practicable, provide for automated scheduling of batch work and processes including backups.
10. On an ongoing basis, enhance processing capabilities and efficiencies through system tuning and other run-time improvements.
11. Operate terminal servers.

- 11.1. Build Application packages, based on customer requirements, for deployment
- 11.2. Deploy the packages based on release schedules.
- 11.3. Provide ongoing coordination and support for DCS Customer Application groups.
- 12. Perform load balancing in coordination with the DCS Customer and any DCS Customer authorized Third Party Vendors.
- 13. Provision, install, operate, support, and in all ways manage application acceleration services, as directed by DIR.
 - 13.1. Provide for the partitioning of the Service such that multiple DCS Customers can securely share the use of application acceleration systems, including the support of multiple organizations and sub-organizations.
 - 13.2. Provide for proactive monitoring and support and in compliance with **Exhibit 2.1.2**.
 - 13.3. Provide reports on the usage of application acceleration services.
- 14. Perform server administration functions, which include the development, establishment, installation, and maintenance of:
 - 14.1. Directories
 - 14.2. Directory structures
 - 14.3. Naming conventions
 - 14.4. File Systems
- 15. Purge records and file old user accounts, as outlined in Section 8 of **Exhibit 2.1.2**.
- 16. Restore archived or deleted files upon Authorized User's request.
- 17. Perform regular monitoring of utilization needs and efficiencies, and report regularly on tuning initiatives.
- 18. Perform or obtain proactive failure trend analysis.
- 19. Produce trend reports to highlight production incidents and problems and establish predetermined action and escalation procedures when batch window incidents and problems are encountered.
- 20. Monitor, verify, and make appropriate adjustments to support proper and timely Application process executions.
- 21. Monitor Applications to proactively prevent or resolve Application performance, degradation or failure where such activities are part of the Service.
- 22. Notify DIR and affected DCS Customers in accordance with the notification procedures in the event that Applications do not execute properly, in accordance with **Exhibit 8**.
- 23. Perform periodic and emergency systems maintenance in accordance with procedures established to minimize the impact to DIR's and DCS Customers' businesses.
- 24. Perform computer shutdowns and restarts, as required, and execute customary utility functions.
 - 24.1. Maintain shutdown and restart order and dependency documentation for all systems and their services/processes for a site.
 - 24.2. Gather and maintain order and dependency information, by DIR and DCS Customer business priorities.

25. Maintain, administer, and provide necessary automated tools and processes for systems management to the extent available in the DIR-approved tool suite or as required to be delivered by the Service Provider elsewhere in the Agreement.
26. Maintain tables, calendars, parameters, and definitions for tools used to automate manual procedures or to automate and improve the quality of the operations.
27. Provide remote monitoring and management for all Equipment.
 - 27.1. Provide on-site Equipment reviews on a scheduled basis for any location, except for Cloud Service Provider Locations, that does not have regularly site visits for installation and maintenance.
28. Maintain and update the operational documentation for all operations procedures and services, including maintaining accurate information about all CIs in the CMS / CMDB.
29. Create and maintain operational documentation for all Applications and Authorized User procedures that affect operations.
30. Provide feedback to DIR and DCS Customers regarding the impact of potential architecture and design changes.
31. Identify opportunities for DIR and DCS Customers to reduce Equipment and Software costs and/or improve system performance.
32. Run or terminate system utilities, depending upon the impact to Authorized Users and only with DIR or DCS Customer approval as appropriate.
33. Proactively monitor and report to DIR and DCS Customers on resource shortages, and report utilization statistics and trends to DIR and DCS Customers on a monthly basis at a level of detail sufficient to identify exceptions.
34. Provide guidance for active prevention of Service performance events (e.g. file CPU, file system level storage, memory, server network interface throughput).
 - 34.1. Provide threshold levels at a server or Application level, per guidelines established through the Technical Solutions Group (TSG).
 - 34.2. Analyze performance metrics and respond proactively to potential problem areas.
35. Suspend, disable, or remove Authorized Users in accordance with procedures and relevant notifications developed and documented with DIR's and DCS Customers' input and approval.
36. Coordinate with DCS Customer LAN support groups as required for LAN services in Remote locations.
37. Install the DIR-provided or DCS Customer-provided servers, gateways, tape, disk, and other Equipment required to maintain the support level necessary to meet ongoing DIR and DCS Customer business requirements, except for Cloud Service Provider locations.
38. Provide, update and maintain a DSL (Definitive Software Library) including references to physical media, license key information, etc. for all server software required to recover or rebuild a server.
39. Install and support sufficient server physical or virtual resources (e.g. data storage, processing capacity, and memory), which may be provided by DIR or DCS Customers.
40. Provide routine administrative services, such as Authorized User and print queue setup, print table setup rights, as well as administration and password administration as requested by DCS Customer.
41. Utilize timing sources as directed by DIR, and as required.

42. Provide Network Time Protocol (NTP) services to DIR and DCS Customers.
43. Audit server rights and privileges on at least a monthly basis and report the results to DIR.
44. Assist individual departments and Authorized Users in lost or damaged file recovery from the Server backups by executing agreed recovery procedures or approved workarounds including defined Recovery Point Objectives (RPO) for the data.
45. Provide assistance in analyzing and correcting all EUC and/or network Problems that may be associated with Server processing.
46. Maintain and update the documentation for all Server operations procedures and services, including maintaining accurate information about all CIs in the CMS / CMDB and relationships between CIs.
47. Provide node/host information, and check and reset ports.
48. Maintain and develop tools and processes to provide automated systems management.
 - 48.1. Provide a standard remote screen sharing service for collaborative work as requested by DIR or DCS Customer.
49. Provide remote Software distribution to Equipment.
50. Provide status and trending reports per **Exhibit 13**, including:
 - 50.1. CPU (average peak utilization for the period)
 - 50.2. Memory (RAM) (average peak utilization for the period)
 - 50.3. Disk (average peak utilization for the period)
 - 50.4. Network Interface Card (NIC) (average peak utilization for the period)
 - 50.5. Servers that have gone above a defined set of thresholds
51. Provide system administration and operational support for high availability.
52. Provide system administration and operational support for high-availability clusters requiring manual and/or automated fail-over methods.
53. Maintain and control spooling to remote sites.
54. Provide technical support for Equipment and Software for remote print locations.
55. Provide operator support for remote print locations.
56. Provide Authorized Users with access to real-time system monitoring information via a portal with profiled access by DIR request (e.g. segregated by DCS Customer).
57. Monitor and alert on thresholds (e.g. dataset or table space capacity events, full log files, file systems, etc.), and provide alerts to DCS Customers as specified in the Service Management Manual.

A.1.1 Physical Security Administration

In addition to the requirements as identified in **Exhibit 17**, Service Provider responsibilities:

1. For Legacy Data Centers for which the Service Provider has operational responsibilities the Service Provider will:
 - 1.1. Recommend supplemental physical security standards and procedures to increase the overall level of security as necessary in the locations and facilities operated by Service Provider.

- 1.2. Implement such supplemental standards and procedures to be consistent with similar security provisions maintained by first tier providers of services that are the same as or similar to the Services.
- 1.3. Obtain DCS Customer's approval prior to implementing any supplemental physical security provisions at DCS Customer facilities.
- 1.4. Comply with DCS Customer's physical security requirements at Legacy Data Centers and Business Offices.

A.2 Production Control and Scheduling

Service Provider responsibilities include:

1. Assume responsibility for production control and scheduling functions for both manual and automated production environments as applicable.
2. Integrate production control and schedule functions as applicable in conformity with DIR's and DCS Customers' requirements.
3. Establish, document, and maintain standards for production jobs.
4. Identify job dependencies, and create and maintain job dependencies on the master scheduling database.
5. Develop, distribute, and obtain DCS Customers' approval of schedules prior to implementation.
6. Coordinate and modify schedules for special requests and comply with DCS Customer priorities.
7. Coordinate resolution of scheduling conflicts.
8. Provide schedule status updates.
9. Proactively prepare for Authorized User deadlines per customized user requirements.
10. Respond expeditiously to requests from DIR or DCS Customers for priority job execution.
11. Promptly notify DCS Customers if special requests will affect the timely completion of other tasks.
12. Prioritize and schedule batch jobs, and report distribution systems (in accordance with DCS Customers' schedule parameters) to optimize the use of processing windows and the scheduled availability of online Applications that are dependent on batch processing, while verifying that batch completion times are met.
13. Take any other necessary steps to prepare Application job streams for production scheduling and execution.
14. Enter program control specifications (parameters) into Application job streams as directed by Authorized Users.
15. Maintain system job streams, including indicating file usages, job dependencies / priorities, and program options available.
16. Perform documentation control functions on all operational documentation.
17. Move programs and documentation to production libraries in accordance with **Exhibit 2.1.2**.
18. Monitor all jobs, scheduled or unscheduled.
19. Start jobs manually where automated processes do not exist or are not available.
20. Investigate and report on all jobs that end or perform abnormally.

21. Where directed, required, or appropriate, restart jobs.
22. Resolve interruptions caused by conditions external to production programs, such as disk or tape problems.
23. Execute re-runs of batch processes as requested by DIR and DCS Customers, and restart jobs according to Service Provider-developed operational procedures (i.e. procedures for successful back-outs, etc.).
24. Create incident and/or problem records and or reports for job abnormalities using the appropriate Tracking System, as described in **Exhibit 2.1.2.**
25. Automate production control and schedule functions wherever possible.

A.3 Technical Support

Service Provider responsibilities include:

1. Provide all technical system support and reporting for operations including:
 - 1.1. Storage management for all media, except for the Cloud Service Provider locations
 - 1.2. System programming
 - 1.3. Capacity planning
 - 1.4. Performance analysis and tuning
2. Install and maintain all system Software products.
3. Develop and install productivity tools/utilities, and perform all required operational modifications for the efficient and proper delivery of the Services.
4. Provide regular monitoring and reporting of system performance, utilization, and efficiency.
5. Ensure the Services effectively utilize the full features and functionality of the hardware and Software within Service Provider responsibility.

A.3.1 General Technical Support

Service Provider responsibilities include the following:

1. Provide appropriate response to incidents and problems and continued support through resolution as required in order to meet scheduled availability.
2. Provide Level 2 Support and Level 3 Support to the Service Desk and/or Authorized Users.
3. Provide technical advice and support (e.g. architecture) to the Application Development and Maintenance (ADM) and Database Administration (DBA) staffs, as required.
 - 3.1. Provide administrative support for Middleware (i.e. MQSeries) on all platforms used in DIR's and DCS Customers' environments.
4. Interface between the groups implementing changes.
5. Monitor data storage media and processor utilization and requirements.
6. Enforce documentation standards in compliance with Service Management Manual directives.
7. Develop, where appropriate, and install productivity tools/utilities, as well as performing all required operational modifications for the efficient and proper delivery of the Services.
8. Develop and maintain technical and functional specifications and requirements for all environments and related interfaces.

9. Provide product research, project support, and advice on Equipment tuning and efficiency improvements, except for the Cloud Service Provider locations.
10. Install, tailor, maintain, and provide ongoing support for System Software products.
11. Install Software according to the Applications' specifications and/or DIR standards as requested by DCS Customer.
12. Distribute Software as efficiently as possible.
13. Manage, prioritize, and coordinate all preventive and remedial maintenance and updates for System Software.
14. Report performance data and resource utilization statistics related to System Software release-level upgrades.
15. Provide consultation support. (For example: product research, project support, Application tuning, and efficiency improvements).
16. Interface and integrate with any additional Third Parties designated by DIR and DCS Customers for the administration and implementation of Address Management (e.g. IP) needed for Services.
17. Provide effective technical support (e.g. installation, patching, event resolution, ADM advice, Third Party Vendor coordination) for software (e.g. Application utilities, middleware) required by the DCS Customers and contained in **Exhibit 8**.
18. Schedule, apply and support security certificates used to secure confidential sessions (SSL) for Internet and Intranet transactions and communications as required by DIR or DCS Customers.
 - 18.1. Coordinate and advise DCS Customers regarding certificates that are embedded in Applications.
 - 18.2. Notify and advise DCS Customers of renewals regarding certificates in timely manner.
19. Install, manage and support Directory Services, including:
 - 19.1. Manage and support authentication using Directory Services, as directed by DIR and DCS Customer.
 - 19.2. Provide and manage trust relationships to existing business-unit domains.
 - 19.3. Remove objects from Directory Services as requested by DIR and DCS Customers.
 - 19.4. Provide LDAP directory resources (Lightweight Directory Access Protocol).
 - 19.5. Provide direction for group policy creation and management.
20. Provide name management (e.g. DNS) as required by DIR and DCS Customers.
 - 20.1. Provide a central support model of name management.
 - 20.2. Manage schema and compliance.
 - 20.3. Administer policies that support consistency.
 - 20.4. Interface and integrate with other providers of name management services (e.g. top-level domain providers, DIR retained name management).
 - 20.5. Appropriately support the delivery of the Services by other DCS Service Providers and Third Party Vendors.

A.3.2 Capacity and Performance Management

The Service Provider is required to assist DIR and DCS Customers in understanding the future business requirements, the organization's operation, and the IT infrastructure, as well as to provide all current and future capacity and performance aspects of the business requirements in a cost effective manner.

The Service Provider responsibilities in addition to those set out in **Exhibit 2.1.2** include:

6. Perform activities required for monitoring and optimizing performance in order to reduce costs or improve Service Levels.
 - 6.1. Report on actions and results per the Service Management Manual.
7. Provide performance monitoring, tuning, and reporting on a defined period basis, including notification to DCS Customers.
8. Provide systems performance reviews and advice.
9. Conduct system performance testing.
10. Perform upgrades to optimize capacity, manage to established thresholds, exceed Service Levels and meet Software architectural requirements.
11. Coordinate with the business partners, Third Party Vendors, other Service Providers, DIR, and DCS Customers as appropriate on projects to install/upgrade hardware and software.
12. Provide and Install necessary tools to perform monitoring and reporting.

A.3.3 Systems Management

Service Provider responsibilities include:

1. Provide, install and utilize tools and processes to allow automated and remote systems management of the Server environment. Processes will include, but are not limited to, Software distribution, backups, performance measurement, tuning, license and asset management, etc.
2. Such tools and processes will include:
 - 2.1. Broadcast Software distribution
 - 2.2. License management tools
 - 2.3. Performance measurement and tuning
 - 2.4. Network and system monitoring and control protocols
 - 2.5. Disaster Recovery/Backup/Business Continuity
 - 2.6. Server administration
 - 2.7. Server management re-configuration (e.g. instance management, virtualization, abstraction layers)
 - 2.8. Automatic alerting
 - 2.9. Configuration Discovery
 - 2.10. Patch Management
 - 2.11. Provide for remote hardware management capabilities in the absence of functioning operating system (such as Appliances) except for hardware provided by Cloud Service Providers.

3. Provide the functionality and necessary Software to allow detection, monitoring, and removal of malicious code and/or unauthorized code from all Servers at a level addressing all common platforms (e.g. file systems, email, instant messaging) generally susceptible to malicious code.

A.4 Database Support and Management

Service Provider responsibilities include:

1. Perform physical database administration functions for the databases required by DIR and DCS Customers, including:
 - 1.1. Storage management Services
 - 1.2. Installation and maintenance, as well as tailoring and monitoring of database Software products
 - 1.3. Backup and recovery
 - 1.4. Assist the DCS Customer in Standards compliance per **Exhibit 8**
 - 1.5. Support
 - 1.6. Security (e.g. segmentation or privacy of information)
 - 1.7. Assist DCS Customer with the import, export, and extractions of data at DCS Customer request.

A.4.1 Database Management

Service Provider responsibilities include:

1. Perform control functions in adherence to Change Management procedures to support systems existing as of the Commencement Date, as well as any planned new systems development.
2. Plan for changes in the size of databases that result from business growth and project implementation, in conjunction with Capacity Management as described in **Exhibit 2.1.2**.
3. Maintain, operate, and upgrade automated monitoring tools to monitor database performance.
4. Perform database shutdowns and restarts.
5. Proactively perform database optimization.
6. Recommend to DCS Customer and perform activities to avoid incidents and performance degradations.

A.4.2 Database Maintenance and Support

Service Provider responsibilities include:

1. Maintain the databases to meet performance standards, to maximize efficiency, and to minimize outages.
2. Maintain, update, and implement database archive tools, processes and procedures to maintain the integrity of the database and recover from an outage or corruption in a timely manner in order to meet DIR's and DCS Customers' business requirements.
 - 2.1. Provide periodic recovery capability testing as requested by DCS Customers per guidelines identified in the Service Management Manual in specific DIR Business Operational sections.

3. Provide physical database management support, including providing backups and restores of data in a timely manner and according to DIR and DCS Customers required schedule and frequency defined in the Service Management Manual.
4. Install, maintain, and support database Software products.
5. Test and implement database environment changes, as approved by DIR or DCS Customers.
6. Monitor database capacity and proactively provide capacity planning to prevent situations caused by lack of capacity (for example: dataset or table space capacity events, full log files, etc.) in coordination with DIR and DCS Customers.
 - 6.1. Monitor, alert and take action on threshold exceptions (e.g. dataset or table space capacity events, full log files, file systems, etc.), and provide alerts to DCS Customers as specified in the Service Management Manual.
 - 6.2. Report on alerts and monitoring to DCS Customer, as specified in the Service Management Manual.
7. In the event of unusual activity (e.g. resource intensive queries),
 - 7.1. Correct situations caused by lack of capacity in a timely manner (e.g. dataset or table space capacity events, full log files, etc.)
 - 7.2. Assist the DCS Customer in analyzing and recommending improvements to prevent future occurrences.
8. Perform the creation, implementation and maintenance of scripts related to the physical database function for all databases, in all supported environments.

A.4.3 Database Administrative Support

Service Provider responsibilities include:

1. Employ database performance analysis to confirm physical database requirements to support DIR's and DCS Customers' business systems.
2. On request, provide DIR, DCS Customer, or its designees with documentation of files generated by the file management systems, including name, utilization statistics, and owning Applications.
3. Provide technical advice to the ADM and DBA groups and assist ADM groups in performing stress testing, and operating system and database performance tuning.
4. Develop, document, and maintain physical database standards and procedures.
5. Participate in evaluating physical database changes and the impact of ADM work. Implement necessary changes, recognizing system and network impact to relevant databases, subject to DIR and DCS Customers' review and approval.
6. Provide technical advice to the ADM and DBA groups related to security and database configuration to support separation of physical and logical DBA roles as they are defined in the Service Management Manual.
7. Provide technical advice to the ADM and DBA groups related to failover and high availability usage and logical DBA design/configuration considerations.

A.5 Online Storage and Backup Management

A.5.1 Storage and Backup Architecture

Service Provider responsibilities include:

1. Provide the architecture, design, and planning processes for the development and installation of a Storage and Backup infrastructure that satisfies the needs of all aspects of the business.
2. Remain current in the knowledge and use of data storage technology and management products.
3. Develop and maintain strategies for the deployment and implementation of Storage and Backup solutions in both Consolidated Data Center, Non-Consolidated Service Locations and Cloud Service Provider locations.
4. Coordinate all aspects of Storage and Backup based architecture, design, and planning throughout DIR.
5. Provide and coordinate a Storage and Backup planning interface to all business units and project managers.

A.5.2 Engineering

Service Provider responsibilities include:

1. Provide a robust and highly available Storage infrastructure, except for Cloud Service Provider locations.
2. Provide a robust and highly available Backup infrastructure. Update the Backup infrastructure as new tools and technology are available that would improve DIR's or DCS Customers' business processes and performance.
3. Investigate incidents and problems that require an in-depth technical understanding per Incident Management and Problem Management process guidelines.
4. Provide in-depth analysis of operations data environment on behalf of availability management, for example, to assist in service outage investigations.
5. Identify opportunities for continual improvement, through knowledge management and constant skill review.
6. Monitor availability and capacity for backup infrastructure, storage and storage media.
7. Educate and train the operational staff in the use of analysis tools and processes, where appropriate.
8. Plan and prepare for changes in capacity requirements.
9. Participate in scheduled disaster recovery tests.
10. Manage Service Provider relationships and provide a technical interface to other project managers and vendors.
11. Provide evaluations and recommendations for new tools and technologies.
12. Establish and maintain the alerting mechanisms and monitoring systems.
13. Perform testing and benchmarking of new infrastructure or tools prior to deployment into production.
14. Create handover documentation, training, diagnostic scripts, and operational procedures for the operations group.

15. Implement performance and configuration tuning of the Storage and Backup infrastructure in conjunction with Capacity Management and Change Management.
16. Establish system tuning and performance processes.
17. Provide appropriate security measures for the Storage and Backup infrastructure.
18. Document the backup, recovery, retention, and archival requirements of DIR and DCS Customers, as specified in the Service Management Manual.

A.5.3 Operations and Processing

Service Provider responsibilities include:

1. Perform successful backups of DIR and DCS Customers systems, in compliance with Service Management Manual.
 - 1.1. Coordinate backup processing with DCS Customers in any situation with the potential to negatively impact operational performance.
2. Remain current in the knowledge and use of data storage technology and management products.
3. Perform online storage tuning.
4. Provide event, warning, alert, and alarm processing and management.
5. Provide resolution of all event, warning, alert, and alarm messages.
 - 5.1. Notify DCS Customers as appropriate on alert notifications.
 - 5.2. Proactively create Incident Records and resolve backup Problems.
6. Interface with the Incident Management and Problem Management processes and liaise with all parties supporting incident and problem resolution.
7. Provide Storage and Backup infrastructure configuration maintenance.
8. Instigate improvement or remedial activities in operational processes under the control of Change Management.
9. Assign and initialize storage as required for performance of the Services.
10. Determine file, data set, and volume placement.
11. Manage the archiving of inactive files and report on online storage directories for review by Operations and DBA staff.
12. Conduct routine monitoring using Software tools to measure the efficiency of online storage access, and take corrective action as needed (including performance adjustments to Equipment and Software, or file placement as required to maximize service).
13. Periodically (but not less than quarterly) retrieve and test all backup media types and verify that the data (including databases) can be restored in a usable fashion.
14. Coordinate with DCS Customers to periodically (but not less than quarterly) perform production recovery testing of DCS Customer data (e.g. file sets, databases) to verify RPO can be met and verify recovery is effective.
15. Provide compression options for disk and tape (e.g. compression on the fly at the server instance vs. compress at the tape drive), except for Cloud Service Provider locations.
16. Support and manage encryption as required by DCS Customer.

17. Provision of partition volume resizing/extending using current technology (e.g. disk imaging, partitioning software) to optimize the process in order to avoid scheduled downtime or recovery risk.

A.5.4 Backup and Recovery Services

Service Provider responsibilities include:

1. Assume responsibility for DIR's and DCS Customers' system data backup and recovery requirements for Non-Consolidated Service Locations, Consolidated Data Centers, and Cloud Service Provider locations.
2. Provide database backup options (e.g. online, offline, compressed) as required by DIR and DCS Customers.
3. Perform backup and recovery functions utilizing available techniques whether standard tool sets or legacy environment tools (e.g. system state backup, fast recovery) options.
4. Provide Backup of Catalogs/Indexes/log files of data backup.
5. Perform systems data backup and recovery of all Service Provider tools and infrastructure components to ensure the integrity and availability of the operational environments which support DCS Customer Applications to meet daily service and DR commitments.
6. Provide reporting on backups and backup infrastructure (e.g. success/failure, schedules, retention, targets, offsite, archive, tape media).
 - 6.1. Ensure backup schedules correctly reflect the Application schedule requirements, retention requirements, and target directory requirements.
 - 6.2. Regularly validate the Application schedule, retention, and target directory requirements.
 - 6.3. Provide the schedule, retention, and target information as implemented in the CMDB and backup systems to the DCS Customer, as requested.
 - 6.4. Review backup schedule and Application schedule with DCS Customer annually.
7. Establish a process by which Authorized Users can request recovery of data or files, and document the process in **Attachment 6-B**.

A.5.5 Administration

Service Provider responsibilities include:

1. Manage online storage thresholds and data archives.
2. Monitor user directories for file inactivity and report monthly.
3. Monitor and maintain file directories and catalogs and report monthly.
4. Provide online storage compaction as needed and as possible within production processing schedules.
5. Provide data migration/archive management, including the migration of media to more current technology to maintain technology currency.
 - 5.1. Coordinate with DCS Customer, as requested, to define and implement disk to tape data archival policies for Application Servers.

- 5.2. Coordinate with DCS Customer, as requested, and in compliance with the Service Management Manual the creation and handling of tapes identified as Do Not Destroy (DND).
6. Provide documentation support and maintenance.
7. Provide and support file system quota management on file servers as required by DCS Customer.

A.6 External Storage Media Management – (Consolidated)

A.6.1 Operations and Processing

Service Provider responsibilities are for the Consolidated Data Centers and include:

1. Coordinate with Data Center Component Provider for operational responsibilities for all External Storage Media management functions, both on-site and off-site, for External Storage Media library operations and administration.
2. Utilize the most efficient and effective storage media, tools, and processes for DCS Customers' data and programs.
3. Coordinate with DCS Service Providers and other Third Party Vendors to recycle media regularly, manage media replacement, and recopy media to provide data integrity and quality.
4. Periodically (but not less than quarterly) coordinate the retrieval and test of all backup media types and verify data can be restored in a usable fashion and report results.
5. Coordinate with the Data Center Component Provider to wipe/erase the data and configuration information resident on media, prior to disposal or re-use, and in accordance with TAC 202.
6. Provide systems administration and support for media libraries and library management systems.
7. Coordinate with the Data Center Component Provider for the provision of all External Media Storage handling (e.g. tape mounts, physical tape library, tape retrieval) functions required in the Consolidated Data Centers.
8. Coordinate the creation and handling of tapes identified as Do Not Destroy (DND) with DCS Customers and the Data Center Component Provider, as requested, and in compliance with the Service Management Manual.

A.6.2 Administration

Service Provider responsibilities are for the Consolidated Data Centers and include:

1. Maintain a database cataloging the archival system for the media libraries.
2. Monitor External Storage Media Equipment in case of malfunction, and initiate corrective action with other DCS Service Providers in accordance with established procedures.
3. Maintain the integrity of External Storage Media libraries system.
4. Monitor External Storage Media for reliability and minimization of read/write errors during the entire period of retention.
5. Monitor and report on External Storage Media usage.
6. Monitor External Storage Media in coordination with the Data Center Component Provider to comply with DIR, DCS Customers and applicable government requirements and reporting.
7. Provide External Storage Media (e.g. cartridges or reel tapes) as required for the Services.

8. Follow, maintain, and update procedures in the Service Management Manual, described in **Attachment 6-B**, which governs cycling/rotation of External Storage Media, External Storage Media management, and External Storage Media retention periods, in accordance with DIR's and DCS Customers' Security Policies, MSI guidelines and with attention to auditing purposes.
9. Manage designated encryption keys for the environment.

A.6.3 Off-Site Media Storage Management

Service Provider responsibilities are for the Consolidated Data Centers and include:

1. Document operational process and procedures for off-site rotation in the Service Management Manual, including coordination with the DCS Customer and Data Center Component Provider as required.
2. Work with DCS Customers and Data Center Component Provider to ensure that off-site rotation is provided for all Service media.

A.7 External Storage Media Management – (Non-Consolidated)

A.7.1 Operations and Processing

Service Provider responsibilities are for the Non-Consolidated Service Locations unless otherwise stated and include:

1. Assume operational responsibilities for all External Storage Media management functions, both on-site and off-site, for External Storage Media library operations and administration in Non-Consolidated Service Locations.
2. Utilize the most efficient and effective storage media, tools, and processes for DCS Customers' data and programs.
3. Recycle media regularly, manage media replacement, and recopy media to provide data integrity and quality.
4. Retrieve External Storage Media from on-site and off-site storage as requested by DIR and DCS Customers or as required in an emergency.
5. Wipe and erase the data and configuration information resident on media, prior to disposal or re-use, and in accordance with TAC 202.
6. Dispose of retired media in an environmentally sound manner after purging any DIR or DCS Customer data using State and/or Federal guidelines/policies prior to disposing of media in accordance with TAC 202.
7. Operate and support media libraries and library management systems as required to provide the Services.
8. Perform External Storage Media handling (e.g. tape mounts, physical tape library, tape retrieval) to support operational activities at sites staffed by Service Provider personnel.
9. Properly clean and maintain Equipment to minimize problems and outages, at intervals established with DIR or in compliance with stated and written specifications.
10. At Business Offices, coordinate with other parties (e.g. Third Party Vendor or DCS Customer) to do:

- 10.1. Establish processes and procedures for proper handling of External Storage Media with the other parties; and
- 10.2. Direct the other parties' personnel to perform External Storage Media mounts.
11. Coordinate the creation and handling of tapes identified as Do Not Destroy (DND) with DCS Customers and the Data Center Component Provider, as requested, and in compliance with the Service Management Manual.
12. Recopy External Storage Media to support minimization of read/write errors, including Refresh to new media per scheduled retirement guidelines, and/or to recover corrupted data.
13. Initialize new External Storage Media.
14. Periodically (but not less than quarterly) retrieve and test all backup media types and verify data can be restored in a usable fashion and report results.

A.7.2 Administration

Service Provider responsibilities are for the Non-Consolidated Service Locations unless otherwise stated and include:

1. Maintain a database cataloging the archival system for the media libraries.
2. Monitor External Storage Media Equipment in case of malfunction, and initiate corrective action in accordance with established procedures.
3. Maintain the integrity of External Storage Media libraries system.
4. Monitor External Storage Media for reliability and minimization of read/write errors during the entire period of retention.
5. Monitor and report on External Storage Media usage and provide usage information to DIR and DCS Customers as set forth in the Service Management Manual.
6. Monitor External Storage Media to comply with DIR, DCS Customers and applicable government requirements and reporting.
7. Provide External Storage Media (e.g. cartridges or reel tapes) as required for the Services.
8. Provide and maintain adequate supplies for the External Storage Media.
9. Follow, maintain, and update procedures in the Service Management Manual, described in **Attachment 6-B**, which governs cycling/rotation of External Storage Media, External Storage Media management, and External Storage Media retention periods, in accordance with DIR's and DCS Customers' Security Policies, MSI guidelines and with attention to auditing purposes.
10. Maintain an existing inventory control system to properly manage External Storage Media in storage and prepare them for shipment to the contingency site.
11. Provide media racks and space for media supporting In-Scope IT environments.
12. Perform Audits of media locations as required per DCS Customer and Service Management Manual Guidelines.
13. Manage designated encryption keys for the environment.

A.7.3 Off-Site Media Storage Management

Service Provider responsibilities are for the Non-Consolidated Service Locations and include:

1. Assume operational responsibility for off-site media storage, for all Non-Consolidated Service Locations as designated by DIR and DCS Customers, including:
 - 1.1. Integrity checking.
 - 1.2. Definition of storage requirements.
 - 1.3. Manage off-site vaulting of data on media as scheduled.
 - 1.4. Cataloging off-site content.
 - 1.5. Retrieving backup tapes.
2. Compliance with DIR's, DCS Customers' and/or applicable government requirements.
3. Develop requirements, procedures, and standards for off-site storage, in consultation with DIR and DCS Customers, and obtain approval from DIR. DIR will have the right to request modifications to such procedures as required.
4. Store External Storage Media and business-recovery-related paper documentation at secure off-site vault storage. Off-site vault storage also includes External Storage Media business recovery functions, such as packaging and transportation to and from storage and contingency sites as defined in **Exhibit 15**.
5. Provide off-site vault storage in a physically and environmentally controlled and protected area with appropriate fire protection and with multiple layers of physical security designed to prevent unauthorized access as defined in **Exhibit 17**.
6. Follow off-site External Storage Media storage procedures, including:
 - 6.1. Provide secure off-site transport containers.
 - 6.2. Prepare media for off-site storage or to go to other Third Parties as requested by DIR or DCS Customers, or as otherwise required.
 - 6.3. Log and track all physical External Storage Media in and out of the Non-Consolidated Service Locations.
 - 6.4. Ship and receive media to and from the off-site storage location(s) on a daily basis, or as required.
 - 6.5. Support ad hoc requests for tape retrieval from off-site locations in a timely manner.
 - 6.6. Maintain the rotation of the External Storage Media that is required for off-site storage.
 - 6.7. Return media as required to the originating DIR or DCS Customer location.
 - 6.8. Transport materials to and from off-site storage in secured environmentally controlled vehicles operated by bonded personnel, or as agreed to by DIR.
 - 6.9. Audit the off-site vendor for compliance and control procedures, and provide an audit report to DIR.
 - 6.10. Maintain the integrity of data shipped to off-site storage.
 - 6.11. Manage Third Party Vendors that provide off-site storage services, and notify DIR and affected DCS Customers of any problems.
 - 6.12. Advise DIR of any modifications to agreements with Third Party Vendors that would improve the efficiency of the Services or otherwise benefit DIR or DCS Customers.
 - 6.13. Manage and provide a daily reconciliation of media that is moved to and from offsite storage to ensure that media flagged for movement is properly moved and logged in the appropriate media tracking and inventory systems.

- 6.14. Manage and provide a reconciliation of all media that is removed from off-site storage following scheduled DR tests and return of media to either off-site storage or the on-site media library.
- 6.15. Provide an emergency media return process.
- 6.16. Comply with, and review compliance with, physical specifications, retention periods, and security.

A.8 Authorized User Support

Service Provider responsibilities include:

1. Provide support, advice, and assistance to DIR Authorized Users in a manner consistent with the guidelines in the Service Management Manual.
2. Perform analysis to provide optimal use of production resources and provide feedback to Authorized Users of those resources.
3. Implement job control and parameter changes for Authorized Users.
4. Provide technical support and administration for various products and Application rollouts.

A.9 Intrusion Prevention

Service Provider's responsibilities include the following for host-based firewall Intrusion Prevention systems:

1. Install, update, and configure Intrusion Systems as requested by DIR or DCS Customers.
2. Monitor all Intrusion Systems from central logging system, and provide appropriate response to alerts from Systems based upon mutually agreed procedures as defined in the Service Management Manual.
 - 2.1. Provide immediate notification and historical reporting to DIR and DCS Customers per guidelines in the Service Management Manual.
3. Install as needed or as directed by DIR or DCS Customers, known high-risk updates as defined by intrusion systems manufacturer to intrusion system Software within 4 hours or less after such updates are made available to Service Provider (or qualified Third-Party Vendors selected by Service Provider) and approved by DIR or DCS Customers.

A.10 Consolidated and Non-Consolidated Data Center Email Services

A.10.1 Email – Procedures

Service Provider responsibilities include:

1. Develop and implement procedures for managing Email Services and email usage.
2. Provide operational training and documentation for supporting Email Services.
3. Design or assist in designing and implementing messaging account administration process and systems (e.g. NetIQ DRA, Terminal Services).
4. Obtain DIR and DCS Customer approval for any new or updated procedures that impact Authorized Users.

A.10.2 Email – Technical Support

Service Provider responsibilities include:

1. Provide evaluation and testing support, including:
 - 1.1. Maintain lab environment for email testing, rebuilding, as required for the standard email platforms.
 - 1.2. Recommend and deploy messaging service Software.
 - 1.3. Evaluate and test compatibility and integration of new products or standards, architecture, and design with existing infrastructure and Applications.
 - 1.4. Test, certify, and coordinate installation, of service packs, hot fixes, Anti-malicious code Software, and definition upgrades for all systems supporting all Email Services (e.g. messaging, instant messaging).
2. Provide technical administration support, including:
 - 2.1. Create administrative and service email accounts and assign roles to these accounts.
 - 2.2. Create and manage the top-level Public Folder and assign rights as requested by DIR and DCS Customers.
 - 2.3. Create, maintain and assign rights to the Distribution Lists and Global Distribution List management.
 - 2.4. Provide support and implementation of Certificates on Email Services systems.
 - 2.5. Initiate and audit DNS records by working with the Telecom and Architecture teams.
3. Provider Email Server support, including:
 - 3.1. Create and manage all server replication topologies.
 - 3.2. Administer and manage all database agents running on server (e.g. Exchange server, Blackberry server)
 - 3.3. Maintain virus protection Software on email servers (shared with data center).
 - 3.4. Coordinate with DCS Customer on emails sent to abuse and postmaster mailboxes, in compliance with Service Management Manual.
 - 3.5. Provide the hardware, software and support of messaging web access (e.g. OWA) from the Internet where resident in infrastructure that is part of the Services.
4. Manage and facilitate the use of Directory Services for Email Services, including managing structures, connections to e-mail systems, facilitating or managing user accounts and excluding directory services solely dedicated to agency end-user applications.
5. Optimize disaster recovery procedures for Email Services.
6. Provide support to Operations, including:
 - 6.1. Develop, implement, and maintain Email Services monitoring and alerting strategy.
 - 6.2. Perform server mailbox load balancing.
 - 6.3. Maintain and troubleshoot internal mail routing.
 - 6.4. Assist End-User Computing support group(s) with troubleshooting of messaging services.
 - 6.5. Work with Third Party and other companies on Internet email delivery issues.
 - 6.6. Escalate messaging issues to Third Party service providers as required.

- 6.7. Perform virus and hoax assessments.
7. Work with Third Party email related systems to provide integration, technical requirements gathering and support for integration with the DCS Customer messaging system.
8. Provide SPAM technical guidance and assistance including:
 - 8.1. Provide technical advice as requested by the DCS Customer for integration and implementation of SPAM appliances or external SPAM solutions.
 - 8.2. Assist in designing and implementing an anti-spam strategy, supporting individual agencies with the approval of DCS Customers.
 - 8.3. Assist DIR and DCS Customers with federated, customizable messaging and internet content filtering that will meet state and federal requirements as identified such as State of Texas Privacy Information, HIPAA and FERPA as well as for DIR and DCS Customers acceptable use policies.
 - 8.4. Work with DIR and DCS Customers in the development and evolution of an enterprise SPAM management architecture.
9. Provide malware (e.g. anti-Virus) protection that is integrated with the email solutions.
10. Perform Email Software installations and upgrades.
11. Provide administration and maintenance of Email Software.

A.10.3 Email – Operations

Service Provider responsibilities include:

1. Manage Email related Directory Services and other related Software/services.
2. Monitor gateways and connectors and troubleshoot both Intranet and Internet email delivery issues.
 - 2.1. Support SMTP mail-relay for some legacy Applications.
 - 2.2. Provide technical support and assistance as required by DIR and DCS Customers.

A.10.4 Authorized User Support

Service Provider responsibilities include:

1. Perform mailbox item restores as requested by DIR and DCS Customers.
2. Provide technical advice and support to DCS Customer in their development of workflow Applications using Directory Services as it relates to email and messaging system integration.
3. Move mailboxes between regions, sectors, divisions, and groups as requested by DCS Customers.
4. Migrate and upgrade mailboxes on the same email product (e.g. Exchange, Groupwise) as requested by DIR and DCS Customers.
 - 4.1. Implement and maintain services such as domain controllers, DNS services (e.g. Active Directory schema) associated with migration or upgrades.
 - 4.2. Install migration tools, including those provided by DIR or DCS Customer.
5. Provide search and data restore as requested by DIR and DCS Customers.

A.11 Enhanced Security Hosted Email Services

Service Provider responsibilities include:

1. Continue all the responsibilities from A.10 Consolidated and Non-Consolidated Data Center Email Services
2. Design and implement enhanced security features necessary to meet regulatory compliance for those DCS Customers whose security needs exceed those of the standard email or Microsoft Office 365 solutions.
 - 2.1. Describe features in the solution proposal presented to the DCS Customer
3. Maintain dedicated infrastructure and labor resources necessary to manage enhanced security hosted email services
4. Provide support for required key management technology.